UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/716,078	11/18/2003	Oleksiy Pikalo	BBNT-P02-097	4787

28120 7590 09/26/2007
ROPES & GRAY LLP
PATENT DOCKETING 39/41
ONE INTERNATIONAL PLACE
BOSTON, MA 02110-2624

EXAMINER	
LOUIE, OSCAR A	
ART UNIT	**PAPER NUMBER**
2136	
MAIL DATE	**DELIVERY MODE**
09/26/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/716,078	Applicant(s) PIKALO ET AL.	
	Examiner Oscar A. Louie	Art Unit 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 18 November 2003.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-62 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-62 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 18 November 2003 is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date 11/03.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

This first non-final action is in response to the original filing of 11/18/2003. Claims 1-62 are pending and have been considered as follows.

Examiner's Note

1. The Applicant appears to be attempting to invoke 35 U.S.C. 112 6th paragraph in Claim 62 by using "means-plus-function" language. However, the Examiner notes that the only "means" for performing these cited functions in the specification appears to be computer program modules. While the claims pass the first test of the three-prong test used to determine invocation of paragraph 6, since no other specific structural limitations are disclosed in the specification, the claims do not meet the other tests of the three-prong test. Therefore, 35 U.S.C. 112 6th paragraph has not been invoked when considering these claims below.

Specification

2. The disclosure is objected to because of the following informalities: Page 1 paragraph 0003 recites "co-pending Application No. ____________." The missing co-pending application number should be included. Appropriate correction is required.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 1-3, 5, 6, 11-13, 15, 17-19, 21, 26, 27, 30, 32-34, 41, 45, 46, 52, 55, & 60-62 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

- Claims 1, 2, 5, 6, 11-13, 15, 17-19, 21, 26, 27, 30, 32-34, 41, 45, 46, 52, 55, & 60-62 recite the limitation(s) "path" sometimes written as "length of QKD path" which are indefinite as to whether the "path" and "length of QKD path" refers to the physical path of the expected fiber optic transmission medium or the directed travel distance of light determined by the incident angle of light projected (i.e. including other factors such as Faraday mirrors, couplers, etc which may all have an effect on the angle of light, thus affecting the travel distance) through the optical transmission medium.
- Claims 1-3, 11-13, 15, 17-19, 27, 30, 32-34, 41, 45, 46, 52, & 60-62 recite the limitation(s) "training symbols" sometimes written as "a sequence of symbols" or "symbols" which are indefinite as to whether these "symbols" are related to timing pulses/information or some other form of information that can be used for timing/modulation or whether "symbols" refers to any light signal with information that may be transmitted over an optical transmission medium (i.e. fiber optics) which may be manipulated or used in the determination of signal adjustments/compensation.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1, 11, 12, 13-17, 26-32, & 41-44 are rejected under 35 U.S.C. 103(a) as being unpatentable over <u>Ahn et al.</u> (US-6160627-A).

Claim 1:

<u>Ahn et al.</u> disclose a method of controlling path length in a quantum cryptographic key distribution (QKD) system, but do not explicitly disclose,

- "receiving training symbols transmitted from a QKD transmitter over a QKD path"
- "controlling a length of the QKD path based on the received training symbols"

however, they do disclose,

- "FIG. 1 illustrates a stabilized optical fiber Mach-Zehnder interferometer in which a transmission wavelength is controlled according to the present invention" [column 3 lines 6-8];
- "for varying the length of the optical fiber" [column 3 line 20];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "receiving training symbols transmitted from a QKD transmitter over a QKD path" and "controlling a length of the QKD path based on the received training symbols," in the invention as disclosed by <u>Ahn et al.</u> since quantum cryptography, which includes quantum cryptographic key distribution, typically has been experimented with and

operated using an optical transmission medium (i.e. fiber optics). Thus, the applicant's claim which appears to be directed towards the operation, adjustment/manipulation, and functionality of optical communications would be applicable to any method, system, apparatus, and medium which utilizes a form of optical communications medium (i.e. in this case quantum cryptography since it is typically implemented with an optical communications medium such as fiber optics). That is, the same rules for optical communications would apply regardless the cryptographic methodology.

Claim 11:

<u>Ahn et al.</u> disclose a system for automatically initializing a length of a quantum cryptographic key distribution (QKD) path in a QKD system, but do not explicitly disclose,

- "a QKD receiver configured to receive training symbols from a QKD transmitter over the QKD path"
- "a phase shifting element disposed on the QKD path"
- "processing logic configured to automatically initialize the length of the QKD path, using the phase shifting element, based on the received training symbols"

however, they do disclose,

- "FIG. 1 illustrates a stabilized optical fiber Mach-Zehnder interferometer in which a transmission wavelength is controlled according to the present invention" [column 3 lines 6-8];
- "an optical fiber phase modulator (fiber stretcher)" [column 3 lines 17-18];
- "for varying the length of the optical fiber" [column 3 line 20];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "a QKD receiver configured to receive training symbols from a QKD transmitter over the QKD path" and "a phase shifting element disposed on the QKD path" and "processing logic configured to automatically initialize the length of the QKD path, using the phase shifting element, based on the received training symbols," in the invention as disclosed by Ahn et al. since quantum cryptography, which includes quantum cryptographic key distribution, typically has been experimented with and operated using an optical transmission medium (i.e. fiber optics). Thus, the applicant's claim which appears to be directed towards the operation, adjustment/manipulation, and functionality of optical communications would be applicable to any method, system, apparatus, and medium which utilizes a form of optical communications medium (i.e. in this case quantum cryptography since it is typically implemented with an optical communications medium such as fiber optics). That is, the same rules for optical communications would apply regardless the cryptographic methodology.

Claim 12:

Ahn et al. disclose a computer-readable medium containing instructions for controlling at least one processor to perform a method of controlling path length in a quantum cryptographic key distribution (QKD) system, but do not explicitly disclose,

- "receiving symbols transmitted from a QKD transmitter over a QKD path"
- "controlling a length of the QKD path based on the received symbols"

however, they do disclose,

- "FIG. 1 illustrates a stabilized optical fiber Mach-Zehnder interferometer in which a transmission wavelength is controlled according to the present invention" [column 3 lines 6-8];
- "for varying the length of the optical fiber" [column 3 line 20];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "receiving symbols transmitted from a QKD transmitter over a QKD path" and "controlling a length of the QKD path based on the received symbols," in the invention as disclosed by Ahn et al. since quantum cryptography, which includes quantum cryptographic key distribution, typically has been experimented with and operated using an optical transmission medium (i.e. fiber optics). Thus, the applicant's claim which appears to be directed towards the operation, adjustment/manipulation, and functionality of optical communications would be applicable to any method, system, apparatus, and medium which utilizes a form of optical communications medium (i.e. in this case quantum cryptography since it is typically implemented with an optical communications medium such as fiber optics). That is, the same rules for optical communications would apply regardless the cryptographic methodology.

Claim 13:

Ahn et al. disclose a method of automatically controlling a path length in a quantum cryptographic key distribution system, the path comprising a first interferometer and a second interferometer, but do not explicitly disclose,

- "employing a phase shifting element in the second interferometer"

- "automatically adjusting the phase shifting element to control the path length based on symbols transmitted over the path"

however, they do disclose,

- "an optical fiber phase modulator (fiber stretcher)" [column 3 lines 17-18];
- "for varying the length of the optical fiber" [column 3 line 20];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "employing a phase shifting element in the second interferometer" and "automatically adjusting the phase shifting element to control the path length based on symbols transmitted over the path," in the invention as disclosed by Ahn et al. since quantum cryptography, which includes quantum cryptographic key distribution, typically has been experimented with and operated using an optical transmission medium (i.e. fiber optics). Thus, the applicant's claim which appears to be directed towards the operation, adjustment/manipulation, and functionality of optical communications would be applicable to any method, system, apparatus, and medium which utilizes a form of optical communications medium (i.e. in this case quantum cryptography since it is typically implemented with an optical communications medium such as fiber optics). That is, the same rules for optical communications would apply regardless the cryptographic methodology.

Claim 14:

Ahn et al. disclose a method of automatically controlling a path length in a quantum cryptographic key distribution system, the path comprising a first interferometer and a second interferometer, as in Claim 13 above, further comprising,

- "the phase shifting element comprises a fiber stretcher" (i.e. "an optical fiber phase modulator (fiber stretcher)" [column 3 lines 17-18].

Claim 15:

Ahn et al. disclose a method of automatically controlling a path length in a quantum cryptographic key distribution system, the path comprising a first interferometer and a second interferometer, as in Claim 14 above, further comprising,

- "adjusting a voltage applied to the fiber stretcher based on the symbols transmitted over the path" (i.e. "an optical fiber phase modulator (fiber stretcher) 40 connected with two light paths of the interferometer between the first and second optical fiber couplers" [column 3 lines 17-19].

Claim 16:

Ahn et al. disclose a method of automatically controlling a path length in a quantum cryptographic key distribution system, the path comprising a first interferometer and a second interferometer, as in Claim 13 above, further comprising,

- "the phase shifting element comprises a phase modulator" (i.e. "an optical fiber phase modulator (fiber stretcher)" [column 3 lines 17-18].

Claim 17:

Ahn et al. disclose a method of automatically controlling a path length in a quantum cryptographic key distribution system, the path comprising a first interferometer and a second interferometer, as in Claim 16 above, further comprising,

- "adjusting a voltage applied to the phase modulator based on the symbols transmitted over the path" (i.e. "an optical fiber phase modulator (fiber stretcher) 40 connected with two light paths of the interferometer between the first and second optical fiber couplers" [column 3 lines 17-19].

Claim 26:

Ahn et al. disclose a system for automatically controlling a path length in a quantum cryptographic key distribution (QKD) system, but do not explicitly disclose,

- "a QKD path including a first interferometer and a second interferometer"
- "a phase shifting element disposed in at least one of the first and second interferometers"
- "processing logic configured to automatically adjust the phase shifting element to control a length of the path"

however, they do disclose,

- "The optical fiber Mach-Zehnder interferometer filter according to the present invention includes a 1.3 .mu.m wavelength turnable laser diode (TLD) 10 (or DFB-LD(Distributed Feedback laser diode)) for implementing a stabilization of an interferometer, first and second 3 dB optical fiber couplers" [column 3 lines 9-14];

- "an optical fiber phase modulator (fiber stretcher) 40 connected with two light paths of the interferometer between the first and second optical fiber couplers" [column 3 lines 17-19];
- "for varying the length of the optical fiber" [column 3 line 20];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "a QKD path including a first interferometer and a second interferometer" and "a phase shifting element disposed in at least one of the first and second interferometers" and "processing logic configured to automatically adjust the phase shifting element to control a length of the path," in the invention as disclosed by Ahn et al. since quantum cryptography, which includes quantum cryptographic key distribution, typically has been experimented with and operated using an optical transmission medium (i.e. fiber optics). Thus, the applicant's claim which appears to be directed towards the operation, adjustment/manipulation, and functionality of optical communications would be applicable to any method, system, apparatus, and medium which utilizes a form of optical communications medium (i.e. in this case quantum cryptography since it is typically implemented with an optical communications medium such as fiber optics). That is, the same rules for optical communications would apply regardless the cryptographic methodology.

Claim 27:

Ahn et al. disclose a method of automatically controlling a path length in a quantum cryptographic key distribution (QKD) system, but do not explicitly disclose,

- "employing a feedback system in the QKD system"

- "automatically controlling the path length, using the feedback system, based on symbols transmitted over the path"

however, they do disclose,

- "feeding-back to the optical fiber phase modulator" [column 3 lines 31-32];
- "for varying the length of the optical fiber" [column 3 line 20];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "employing a feedback system in the QKD system" and "automatically controlling the path length, using the feedback system, based on symbols transmitted over the path," in the invention as disclosed by Ahn et al. since quantum cryptography, which includes quantum cryptographic key distribution, typically has been experimented with and operated using an optical transmission medium (i.e. fiber optics). Thus, the applicant's claim which appears to be directed towards the operation, adjustment/manipulation, and functionality of optical communications would be applicable to any method, system, apparatus, and medium which utilizes a form of optical communications medium (i.e. in this case quantum cryptography since it is typically implemented with an optical communications medium such as fiber optics). That is, the same rules for optical communications would apply regardless the cryptographic methodology.

Claim 28:

Ahn et al. disclose a method of automatically controlling a path length in a quantum cryptographic key distribution (QKD) system, as in Claim 27 above, further comprising,

- "the feedback system comprises a phase shifting element" (i.e. "an optical fiber phase modulator (fiber stretcher)") [column 3 lines 17-18].

Claim 29:

Ahn et al. disclose a method of automatically controlling a path length in a quantum cryptographic key distribution (QKD) system, as in Claim 28 above, further comprising,

- "the phase shifting element comprises a fiber stretcher" (i.e. "an optical fiber phase modulator (fiber stretcher)") [column 3 lines 17-18].

Claim 30:

Ahn et al. disclose a method of automatically controlling a path length in a quantum cryptographic key distribution (QKD) system, as in Claim 29 above, further comprising,

- "adjusting a voltage applied to the fiber stretcher based on the symbols transmitted over the path" (i.e. "an optical fiber phase modulator (fiber stretcher) 40 connected with two light paths of the interferometer between the first and second optical fiber couplers" [column 3 lines 17-19].

Claim 31:

Ahn et al. disclose a method of automatically controlling a path length in a quantum cryptographic key distribution (QKD) system, as in Claim 28 above, further comprising,

- "the phase shifting element comprises a phase modulator" (i.e. "an optical fiber phase modulator (fiber stretcher)") [column 3 lines 17-18].

Claim 32:

Ahn et al. disclose a method of automatically controlling a path length in a quantum cryptographic key distribution (QKD) system, as in Claim 31 above, further comprising,

- "adjusting a voltage applied to the phase modulator based on the symbols transmitted over the path" (i.e. "an optical fiber phase modulator(fiber stretcher) 40 connected with two light paths of the interferometer between the first and second optical fiber couplers" [column 3 lines 17-19].

Claim 41:

Ahn et al. disclose a quantum cryptographic key distribution (QKD) endpoint, but do not explicitly disclose,

- "a QKD receiver configured to receive symbols transmitted over a QKD path"
- "a feedback system configured to control a length of the QKD path based on the received symbols"

however, they do disclose,

- "FIG. 1 illustrates a stabilized optical fiber Mach-Zehnder interferometer in which a transmission wavelength is controlled according to the present invention" [column 3 lines 6-8];
- "for varying the length of the optical fiber" [column 3 line 20];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "a QKD receiver configured to receive symbols transmitted over a QKD path" and "a feedback system configured to control a length of the QKD path based on the received symbols," in the invention as disclosed by Ahn et al. since quantum

cryptography, which includes quantum cryptographic key distribution, typically has been experimented with and operated using an optical transmission medium (i.e. fiber optics). Thus, the applicant's claim which appears to be directed towards the operation, adjustment/manipulation, and functionality of optical communications would be applicable to any method, system, apparatus, and medium which utilizes a form of optical communications medium (i.e. in this case quantum cryptography since it is typically implemented with an optical communications medium such as fiber optics). That is, the same rules for optical communications would apply regardless the cryptographic methodology.

Claim 42:

Ahn et al. disclose a quantum cryptographic key distribution (QKD) endpoint, as in Claim 41 above, further comprising,

- "the feedback system comprises a phase shifting element" (i.e. "an optical fiber phase modulator (fiber stretcher)") [column 3 lines 17-18].

Claim 43:

Ahn et al. disclose a quantum cryptographic key distribution (QKD) endpoint, as in Claim 42 above, further comprising,

- "the phase shifting element comprises a fiber stretcher" (i.e. "an optical fiber phase modulator (fiber stretcher)") [column 3 lines 17-18].

Claim 44:

Ahn et al. disclose a quantum cryptographic key distribution (QKD) endpoint, as in Claim 42 above, further comprising,

- "the phase shifting element comprises a phase modulator" (i.e. "an optical fiber phase modulator (fiber stretcher)") [column 3 lines 17-18].

7. Claims 52-59, 61 & 62 are rejected under 35 U.S.C. 103(a) as being unpatentable over Page (US-5157461-A).

Claim 52:

Page discloses a method of controlling a length of a path in a quantum cryptographic key distribution (QKD) system, but does not explicitly disclose,

- "determining probabilities associated with a plurality of detection events"
- "the plurality of detection events being associated with a sequence of symbols received over the path in the QKD system"
- "controlling the length of the path based on the determined probabilities"

however, Page does disclose,

- "an "a priori" mean square estimation error is computed as a function of rate correlation time, previous mean square estimation error computations, and the statistical effects of the previously-described residual noise" [column 18 lines 20-24];
- "the detection circuit means and responsive to the intensity signal for generating output signals corresponding at least in part to the rate of angular rotation" [column 26 lines 43-46];

- "a sequential Kalman filter can provide optimal estimates of the true value of the modulator drive voltage corresponding to the central peak of the intensity signal S, even with substantially noisy measurements of this peak location" [column 17 lines 51-55];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "determining probabilities associated with a plurality of detection events" and "the plurality of detection events being associated with a sequence of symbols received over the path in the QKD system" and "controlling the length of the path based on the determined probabilities," in the invention as disclosed by Page since quantum cryptography, which includes quantum cryptographic key distribution, typically has been experimented with and operated using an optical transmission medium (i.e. fiber optics). Thus, the applicant's claim which appears to be directed towards the operation, adjustment/manipulation, and functionality of optical communications would be applicable to any method, system, apparatus, and medium which utilizes a form of optical communications medium (i.e. in this case quantum cryptography since it is typically implemented with an optical communications medium such as fiber optics). That is, the same rules for optical communications would apply regardless the cryptographic methodology.

Claim 53:

Page discloses a method of controlling a length of a path in a quantum cryptographic key distribution (QKD) system, as in Claim 52 above, further comprising,

- "the probabilities comprise conditional probabilities" (i.e. "the statistical effects of the previously-described residual noise") [column 18 lines 23-24].

Claim 54:

Page discloses a method of controlling a length of a path in a quantum cryptographic key distribution (QKD) system, as in Claim 52 above, further comprising,

- "estimating a phase error based on the determined probabilities" (i.e. "an "a priori" mean square estimation error is computed as a function of rate correlation time, previous mean square estimation error computations, and the statistical effects of the previously-described residual noise") [column 18 lines 20-24].

Claim 55:

Page discloses a method of controlling a length of a path in a quantum cryptographic key distribution (QKD) system, as in Claim 54 above, further comprising,

- "controlling the path length of the QKD path further based on the estimated phase error" (i.e. "a sequential Kalman filter can provide optimal estimates of the true value of the modulator drive voltage corresponding to the central peak of the intensity signal S, even with substantially noisy measurements of this peak location" [column 17 lines 51-55].

Claim 56:

Page discloses a method of controlling a length of a path in a quantum cryptographic key distribution (QKD) system, as in Claim 54 above, further comprising,

- "performing a least squares estimation of the phase error using the determined probabilities" (i.e. "an "a priori" mean square estimation error is computed as a function of rate correlation time, previous mean square estimation error computations, and the statistical effects of the previously-described residual noise") [column 18 lines 20-24].

Claim 57:

Page discloses a method of controlling a length of a path in a quantum cryptographic key distribution (QKD) system, as in Claim 54 above, further comprising,

- "employing at least one Kalman filter to estimate the phase error" (i.e. "a sequential Kalman filter can provide optimal estimates of the true value of the modulator drive voltage corresponding to the central peak of the intensity signal S, even with substantially noisy measurements of this peak location" [column 17 lines 51-55].

Claim 58:

Page discloses a method of controlling a length of a path in a quantum cryptographic key distribution (QKD) system, as in Claim 54 above, further comprising,

- "performing a robust least squares estimation of the phase error using the determined probabilities" (i.e. "a sequential Kalman filter can provide optimal estimates of the true value of the modulator drive voltage corresponding to the central peak of the intensity signal S, even with substantially noisy measurements of this peak location" [column 17 lines 51-55].

Claim 59:

Page discloses a method of controlling a length of a path in a quantum cryptographic key distribution (QKD) system, as in Claim 58 above, further comprising,

- "at least one of least absolute residuals and Bisquare weight" (i.e. "These detections can be accomplished by means of conventional methods such as "curve fitting" utilizing the principles of "linear least squares" as commonly known in the art") [column 16 lines 51-54].

Claims 61 & 62:

Page discloses a computer-readable medium containing instructions for controlling at least one processor to perform a method of controlling a length of a path in a quantum cryptographic key distribution (QKD) system and a system for controlling a length of a path in a quantum cryptographic key distribution (QKD) system, but does not explicitly disclose,

- "(means for) determining probabilities associated with a plurality of detection events"
- "the plurality of detection events being associated with a sequence of symbols received over the path in the QKD system"
- "(means for) controlling the length of the path based on the determined probabilities"

however, Page does disclose,

- "an "a priori" mean square estimation error is computed as a function of rate correlation time, previous mean square estimation error computations, and the statistical effects of the previously-described residual noise" [column 18 lines 20-24];
- "the detection circuit means and responsive to the intensity signal for generating output signals corresponding at least in part to the rate of angular rotation" [column 26 lines 43-46];
- "These detections can be accomplished by means of conventional methods such as "curve fitting" utilizing the principles of "linear least squares" as commonly known in the art" [column 16 lines 51-54];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "determining probabilities associated with a plurality of detection events" and "the plurality of detection events being associated with a sequence of symbols received over the path in the QKD system" and "controlling the length of the path based on the determined probabilities," in the invention as disclosed by Page since quantum cryptography, which includes quantum cryptographic key distribution, typically has been experimented with and operated using an optical transmission medium (i.e. fiber optics). Thus, the applicant's claim which appears to be directed towards the operation, adjustment/manipulation, and functionality of optical communications would be applicable to any method, system, apparatus, and medium which utilizes a form of optical communications medium (i.e. in this case quantum cryptography since it is typically implemented with an optical communications medium such as fiber optics). That is, the same rules for optical communications would apply regardless the cryptographic methodology.

8. Claims 2-10, 18-25, 33-40, 45-51, & 60 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ahn et al. (US-6160627-A) in view of Page (US-5157461-A).

Claim 2:

Ahn et al. disclose a method of controlling path length in a quantum cryptographic key distribution (QKD) system, as in Claim 1 above, but do not disclose,

- "estimating a phase error associated with transmission of the training symbols over the QKD path"

however, Page does disclose,

- “an "a priori" mean square estimation error is computed as a function of rate correlation time, previous mean square estimation error computations, and the statistical effects of the previously-described residual noise” [column 18 lines 20-24];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant’s invention to include, “estimating a phase error associated with transmission of the training symbols over the QKD path,” in the invention as disclosed by Ahn et al. for the purposes of deriving an optimal estimate of the central peak modulator voltage.

Claim 3:

Ahn et al. disclose a method of controlling path length in a quantum cryptographic key distribution (QKD) system, as in Claim 2 above, further comprising,

- “determining probabilities of detection events associated with the received training symbols” (i.e. “the detection circuit means and responsive to the intensity signal for generating output signals corresponding at least in part to the rate of angular rotation”) [column 26 lines 43-46].

Claim 4:

Ahn et al. disclose a method of controlling path length in a quantum cryptographic key distribution (QKD) system, as in Claim 3 above, further comprising,

- “estimating the phase error based on the determined probabilities” (i.e. “an "a priori" mean square estimation error is computed as a function of rate correlation time, previous mean square estimation error computations, and the statistical effects of the previously-described residual noise”) [column 18 lines 20-24].

Claim 5:

Ahn et al. disclose a method of controlling path length in a quantum cryptographic key distribution (QKD) system, as in Claim 2 above, further comprising,

- "controlling the length of the QKD path based on the estimated phase error" (i.e. "a sequential Kalman filter can provide optimal estimates of the true value of the modulator drive voltage corresponding to the central peak of the intensity signal S, even with substantially noisy measurements of this peak location") [column 17 lines 51-55].

Claim 6:

Ahn et al. disclose a method of controlling path length in a quantum cryptographic key distribution (QKD) system, as in Claim 4 above, further comprising,

- "controlling the length of the QKD path based on the estimated phase error" (i.e. "a sequential Kalman filter can provide optimal estimates of the true value of the modulator drive voltage corresponding to the central peak of the intensity signal S, even with substantially noisy measurements of this peak location") [column 17 lines 51-55].

Claim 7:

Ahn et al. disclose a method of controlling path length in a quantum cryptographic key distribution (QKD) system, as in Claim 4 above, further comprising,

- "performing a least squares estimation of the phase error using the determined probabilities" (i.e. "an "a priori" mean square estimation error is computed as a function of rate correlation time, previous mean square estimation error computations, and the statistical effects of the previously-described residual noise") [column 18 lines 20-24].

Claim 8:

Ahn et al. disclose a method of controlling path length in a quantum cryptographic key distribution (QKD) system, as in Claim 2 above, further comprising,

- "employing at least one Kalman filter to estimate the phase error" (i.e. "a sequential Kalman filter can provide optimal estimates of the true value of the modulator drive voltage corresponding to the central peak of the intensity signal S, even with substantially noisy measurements of this peak location") [column 17 lines 51-55].

Claim 9:

Ahn et al. disclose a method of controlling path length in a quantum cryptographic key distribution (QKD) system, as in Claim 4 above, further comprising,

- "performing a robust least squares estimation of the phase error using the determined probabilities" (i.e. "a sequential Kalman filter can provide optimal estimates of the true value of the modulator drive voltage corresponding to the central peak of the intensity signal S, even with substantially noisy measurements of this peak location") [column 17 lines 51-55].

Claim 10:

Ahn et al. disclose a method of controlling path length in a quantum cryptographic key distribution (QKD) system, as in Claim 9 above, further comprising,

- "at least one of least absolute residuals and Bisquare weights" (i.e. "These detections can be accomplished by means of conventional methods such as "curve fitting" utilizing the principles of "linear least squares" as commonly known in the art") [column 16 lines 51-54].

Claim 18:

Ahn et al. disclose a method of automatically controlling a path length in a quantum cryptographic key distribution system, the path comprising a first interferometer and a second interferometer, as in Claim 13 above, but do not disclose,

- "estimating a phase error associated with symbols transmitted over the path"

however, Page does disclose,

- "an "a priori" mean square estimation error is computed as a function of rate correlation time, previous mean square estimation error computations, and the statistical effects of the previously-described residual noise" [column 18 lines 20-24];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "estimating a phase error associated with symbols transmitted over the path," in the invention as disclosed by Ahn et al. for the purposes of deriving an optimal estimate of the central peak modulator voltage.

Claim 19:

Ahn et al. disclose a method of automatically controlling a path length in a quantum cryptographic key distribution system, the path comprising a first interferometer and a second interferometer, as in Claim 18 above, further comprising,

- "determining probabilities of detection events associated with the symbols transmitted over the path" (i.e. "the detection circuit means and responsive to the intensity signal for generating output signals corresponding at least in part to the rate of angular rotation") [column 26 lines 43-46].

Claim 20:

Ahn et al. disclose a method of automatically controlling a path length in a quantum cryptographic key distribution system, the path comprising a first interferometer and a second interferometer, as in Claim 19 above, further comprising,

- "estimating the phase error based on the determined probabilities" (i.e. "an "a priori" mean square estimation error is computed as a function of rate correlation time, previous mean square estimation error computations, and the statistical effects of the previously-described residual noise" [column 18 lines 20-24].

Claim 21:

Ahn et al. disclose a method of automatically controlling a path length in a quantum cryptographic key distribution system, the path comprising a first interferometer and a second interferometer, as in Claim 18 above, further comprising,

- "the phase shifting element is automatically adjusted to control the path length further based on the estimated phase error" (i.e. "a sequential Kalman filter can provide optimal estimates of the true value of the modulator drive voltage corresponding to the central peak of the intensity signal S, even with substantially noisy measurements of this peak location" [column 17 lines 51-55].

Claim 22:

Ahn et al. disclose a method of automatically controlling a path length in a quantum cryptographic key distribution system, the path comprising a first interferometer and a second interferometer, as in Claim 20 above, further comprising,

- "performing a least squares estimation of the phase error using the determined probabilities" (i.e. "an "a priori" mean square estimation error is computed as a function of rate correlation time, previous mean square estimation error computations, and the statistical effects of the previously-described residual noise" [column 18 lines 20-24].

Claim 23:

Ahn et al. disclose a method of automatically controlling a path length in a quantum cryptographic key distribution system, the path comprising a first interferometer and a second interferometer, as in Claim 18 above, further comprising,

- "employing at least one Kalman filter to estimate the phase error" (i.e. "a sequential Kalman filter can provide optimal estimates of the true value of the modulator drive voltage corresponding to the central peak of the intensity signal S, even with substantially noisy measurements of this peak location" [column 17 lines 51-55].

Claim 24:

Ahn et al. disclose a method of automatically controlling a path length in a quantum cryptographic key distribution system, the path comprising a first interferometer and a second interferometer, as in Claim 20 above, further comprising,

- "performing a robust least squares estimation of the phase error using the determined probabilities" (i.e. "a sequential Kalman filter can provide optimal estimates of the true

value of the modulator drive voltage corresponding to the central peak of the intensity signal S, even with substantially noisy measurements of this peak location" [column 17 lines 51-55].

Claim 25:

Ahn et al. disclose a method of automatically controlling a path length in a quantum cryptographic key distribution system, the path comprising a first interferometer and a second interferometer, as in Claim 24 above, further comprising,

- "at least one of least absolute residuals and Bisquare weights" (i.e. "These detections can be accomplished by means of conventional methods such as "curve fitting" utilizing the principles of "linear least squares" as commonly known in the art") [column 16 lines 51-54].

Claim 33:

Ahn et al. disclose a method of automatically controlling a path length in a quantum cryptographic key distribution (QKD) system, as in Claim 27 above, but do not disclose,

- "estimating a phase error associated with symbols transmitted over the path"

however, Page does disclose,

- "an "a priori" mean square estimation error is computed as a function of rate correlation time, previous mean square estimation error computations, and the statistical effects of the previously-described residual noise" [column 18 lines 20-24];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "estimating a phase error associated with symbols transmitted over the path," in the invention as disclosed by Ahn et al. for the purposes of deriving an optimal estimate of the central peak modulator voltage.

Claim 34:

Ahn et al. disclose a method of automatically controlling a path length in a quantum cryptographic key distribution (QKD) system, as in Claim 33 above, further comprising,

- "determining probabilities of detection events associated with the symbols transmitted over the path" (i.e. "the detection circuit means and responsive to the intensity signal for generating output signals corresponding at least in part to the rate of angular rotation") [column 26 lines 43-46].

Claim 35:

Ahn et al. disclose a method of automatically controlling a path length in a quantum cryptographic key distribution (QKD) system, as in Claim 34 above, further comprising,

- "estimating the phase error based on the determined probabilities" (i.e. "an "a priori" mean square estimation error is computed as a function of rate correlation time, previous mean square estimation error computations, and the statistical effects of the previously-described residual noise") [column 18 lines 20-24].

Claim 36:

Ahn et al. disclose a method of automatically controlling a path length in a quantum cryptographic key distribution (QKD) system, as in Claim 33 above, further comprising,

- "the path length is automatically controlled further based on the estimated phase error" (i.e. "a sequential Kalman filter can provide optimal estimates of the true value of the modulator drive voltage corresponding to the central peak of the intensity signal S, even with substantially noisy measurements of this peak location") [column 17 lines 51-55].

Claim 37:

Ahn et al. disclose a method of automatically controlling a path length in a quantum cryptographic key distribution (QKD) system, as in Claim 35 above, further comprising,

- "performing a least squares estimation of the phase error using the determined probabilities" (i.e. "an "a priori" mean square estimation error is computed as a function of rate correlation time, previous mean square estimation error computations, and the statistical effects of the previously-described residual noise") [column 18 lines 20-24].

Claim 38:

Ahn et al. disclose a method of automatically controlling a path length in a quantum cryptographic key distribution (QKD) system, as in Claim 35 above, further comprising,

- "employing at least one Kalman filter to estimate the phase error" (i.e. "a sequential Kalman filter can provide optimal estimates of the true value of the modulator drive voltage corresponding to the central peak of the intensity signal S, even with substantially noisy measurements of this peak location") [column 17 lines 51-55].

Claim 39:

Ahn et al. disclose a method of automatically controlling a path length in a quantum cryptographic key distribution (QKD) system, as in Claim 35 above, further comprising,

- "performing a robust least squares estimation of the phase error using the determined probabilities" (i.e. "a sequential Kalman filter can provide optimal estimates of the true value of the modulator drive voltage corresponding to the central peak of the intensity signal S, even with substantially noisy measurements of this peak location") [column 17 lines 51-55].

Claim 40:

Ahn et al. disclose a method of automatically controlling a path length in a quantum cryptographic key distribution (QKD) system, as in Claim 39 above, further comprising,

- "at least one of least absolute residuals and Bisquare weights" (i.e. "These detections can be accomplished by means of conventional methods such as "curve fitting" utilizing the principles of "linear least squares" as commonly known in the art") [column 16 lines 51-54].

Claim 45:

Ahn et al. disclose a quantum cryptographic key distribution (QKD) endpoint, as in Claim 41 above, but do not disclose,

- "estimate a phase error associated with the symbols transmitted over the QKD path based on the received symbols"

however, Page does disclose,

- “an "a priori" mean square estimation error is computed as a function of rate correlation time, previous mean square estimation error computations, and the statistical effects of the previously-described residual noise” [column 18 lines 20-24];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant’s invention to include, “estimate a phase error associated with the symbols transmitted over the QKD path based on the received symbols,” in the invention as disclosed by Ahn et al. for the purposes of deriving an optimal estimate of the central peak modulator voltage.

Claim 46:

Ahn et al. disclose a quantum cryptographic key distribution (QKD) endpoint, as in Claim 45 above, further comprising,

- “determine probabilities of detection events associated with the symbols transmitted over the QKD path” (i.e. “the detection circuit means and responsive to the intensity signal for generating output signals corresponding at least in part to the rate of angular rotation”) [column 26 lines 43-46].

Claim 47:

Ahn et al. disclose a quantum cryptographic key distribution (QKD) endpoint, as in Claim 46 above, further comprising,

- “estimate the phase error based on the determined probabilities” (i.e. “an "a priori" mean square estimation error is computed as a function of rate correlation time, previous mean square estimation error computations, and the statistical effects of the previously-described residual noise”) [column 18 lines 20-24].

Claim 48:

Ahn et al. disclose a quantum cryptographic key distribution (QKD) endpoint, as in Claim 45 above, further comprising,

- "the estimation system comprises a least squares estimator" (i.e. "a sequential Kalman filter can provide optimal estimates of the true value of the modulator drive voltage corresponding to the central peak of the intensity signal S, even with substantially noisy measurements of this peak location") [column 17 lines 51-55].

Claim 49:

Ahn et al. disclose a quantum cryptographic key distribution (QKD) endpoint, as in Claim 45 above, further comprising,

- "the estimation system comprises at least one Kalman filter" (i.e. "a sequential Kalman filter can provide optimal estimates of the true value of the modulator drive voltage corresponding to the central peak of the intensity signal S, even with substantially noisy measurements of this peak location") [column 17 lines 51-55].

Claim 50:

Ahn et al. disclose a quantum cryptographic key distribution (QKD) endpoint, as in Claim 45 above, further comprising,

- "estimation system comprises a robust least squares estimator" (i.e. "a sequential Kalman filter can provide optimal estimates of the true value of the modulator drive voltage corresponding to the central peak of the intensity signal S, even with substantially noisy measurements of this peak location") [column 17 lines 51-55].

Claim 51:

Ahn et al. disclose a quantum cryptographic key distribution (QKD) endpoint, as in Claim 50 above, further comprising,

- "the robust least squares estimator employs at least one of least absolute residuals and Bisquare weights" (i.e. "These detections can be accomplished by means of conventional methods such as "curve fitting" utilizing the principles of "linear least squares" as commonly known in the art") [column 16 lines 51-54].

Claim 60:

Ahn et al. disclose a quantum cryptographic key distribution (QKD) endpoint comprising,

- "a QKD receiver configured to receive a sequence of symbols transmitted over a QKD path" (i.e. "FIG. 1 illustrates a stabilized optical fiber Mach-Zehnder interferometer in which a transmission wavelength is controlled according to the present invention") [column 3 lines 6-8];
- "a phase shifting element disposed on the QKD path" (i.e. "an optical fiber phase modulator (fiber stretcher) 40 connected with two light paths of the interferometer between the first and second optical fiber couplers") [column 3 lines 17-19];

but do not disclose,

- "processing logic configured to: determine conditional probabilities associated with a plurality of detection events"
- "the plurality of detection events being associated with the sequence of symbols"
- "processing logic configured to: adjust the phase shifting element to control a length of the QKD path based on the determined conditional probabilities"

however, Page does disclose,

- "an "a priori" mean square estimation error is computed as a function of rate correlation time, previous mean square estimation error computations, and the statistical effects of the previously-described residual noise" [column 18 lines 20-24];
- "the detection circuit means and responsive to the intensity signal for generating output signals corresponding at least in part to the rate of angular rotation" [column 26 lines 43-46];
- "a sequential Kalman filter can provide optimal estimates of the true value of the modulator drive voltage corresponding to the central peak of the intensity signal S, even with substantially noisy measurements of this peak location" [column 17 lines 51-55];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "processing logic configured to: determine conditional probabilities associated with a plurality of detection events" and "the plurality of detection events being associated with the sequence of symbols" and "processing logic configured to: adjust the phase shifting element to control a length of the QKD path based on the determined conditional probabilities," in the invention as disclosed by Ahn et al. for the purposes of deriving an optimal estimate of the central peak modulator voltage.

Conclusion

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Examiner Oscar Louie whose telephone number is 571-270-1684. The examiner can normally be reached Monday through Thursday from 7:30 AM to 4:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami, can be reached at 571-272-4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

OAL
09/19/2007

Nasser Moazzami
Supervisory Patent Examiner

9/20/07